Kilifi MIMcom workshop - minutes

DAY 1

Workshop Objectives – Open session
- Bandwidth use and control
- Using existing tools to answer users questions
- Hacker Security
- Configuration of servers, firewalls and routers
- Access policy (Security and Bandwidth control)
- Wireless security
- What do 'we' want RSS to do for us?
- Data sharing (Databases on the network)
- VoFR/VoIP
- What DB's are available? (user oriented)
- Local Security / Active Server pages

Bandwidth Control – Erik Schoute/Tom Oluoch/Mark Bennett
- inbound and outbound b/w differs between sites
- sites tend to use whatever b/w they have
- Nairobi shifts the most
- Ping time SD is measure of how much (%) of their b/w they use

Site findings

Kisian	MSN
	Hotmail
Kilifi	Soccernet.com
	Google
	Utilisation ~ 95%
	Rx – 59%
	Long ping times
Noguchi	Av. Ping time 670 ms
	Utilisation –
	MSN – Most visited (Home page in most cases)
Navrongo	Av. Ping 670 ms
	Max Ping varies
	Most visited – Hotmail, MSN, Yahoo
Nairobi	Hotmail, Yahoo, Symantec
Amani	unknown
Ifakara	similar to the rest
Entebbe	Av Ping time 520
	Top site – soccernet.com, iBank, Barclays.com
Mbita	similar to the rest

Observations / problems
- Hotmail/Yahoo are the main b/w users
- GroupWise/Exchange Licence shortage can force users to use Hotmail accounts
- Private mail is being done through Hotmail
- Fear that MIMCom accounts are monitored makes users use Hotmail accounts
- Visiting&travelling scientists use Hotmail
- Connections outside firewall
- Inadequate user training: users don't know about the consequences Hotmail etc has for the Internet link
- Many users sharing a PC (More users than PCs) makes use of Outlook or Outlook Express more difficult
- Sys Admins not in control of all access points on the LAN, there are users online that Sysop is not even aware off

- Subscription to junk mail sites, sometimes without user wanting it
- Bonzi buddy and other automatic sites use b/w
- Internet mail accounts as a source of viruses

Solutions
- Using a single or just a few PC's for Yahoo/Hotmail
- Blocking adverts from sites wills ave b/w even on Hotmail / Yahoo pages
- Proxy server in each site (but doesn't work for Hotmail etc)
- User training / sensitisation. Personal interaction with the users to inform them of consequences
- Stop users changing their own PCs configuration by using accounts under W2k
- Write a policy and enforce it (support memo from management/directors)
- Allow limited use of Yahoo/Hotmail – centrally controlled
- Change browsers' default/home page because the MSN page refreshes automatically
- Blocking inappropriate sites (locally and centally)
- Monitor frequently visited sites for a month and propose the ones to block
- Use POP3 to get mail from Hotmail etc.

Action
- RSS will resume blocking adverts
- Start moving users from Hotmail web interface to POP3 to get mail from Hotmail.
- Train / inform / sensitisize users about b/w usage
- Check the Sawmill stats. In 4 weeks time give Mark a list of inappropriate websites to block. Mark will compile a list that is fed back to the sites. The sites' management then decides what to block.

DAY 2

Introduction of new sites

Blantyre:

Connected to an ISP via RF link.
Information rate – 64K, plans to upgrade to 128K
Approx. 200 PCs.

Entebbe:

Prevously used radio link through the airport, breezecom adapter to an ISP with a dedicated 64K, which in reality had a throughput of 32K.

6 servers, 5 currently operational
1 PDC running NT server, the rest run BDC
One of the applicaton server running the Library …
RAS is actively used
Wireless access point for laptop users
Serves Mulago hospital and Tororo connected via dial-up.
Approx 120 connected computers
Efficient antivirus software (antigen), scheduled update every night.
No major problems with the users control

Mbita

ICIPE was previously connected via an unreliable dial-up to the head office. Used Mac servers. Telephone link is very unreliable.

50 PCs and Macs and two servers running Win2k,
One server runs Exchange, etc
One server hosts applications SPSS, SAS and Endnote, it also acts as the file server.
Wireless using LinkSys and the Mac wireless application
LanScan for tracking user activity.
Sawmill to monitor bandwidth utilisation
Virus Scan definition files updated nightly.

SMAC Activities – Chris Olola

Severe Malaria in African Children Clinical Network. Currently conducting two multi-centre clinical studies, namely Pigment study and Pentoxyfilin (PTX) study. The regional data coordinator is based in Kilifi. External collaborators – Michigan State and Havard Universities.

Set up in January 1997 and covers five sites in Kenya, Malawi, Gambia, Ghana and Gabon.
Updates of data from sites are contrally updated monthly.
Analysis done in Kilifi and verified in Havard
Efficient communication exists only in Kilifi and Malawi. The rest of the sites use dial-up.
A database existed only in Kilifi and the Data Coordinator has gone round setting up databases at all SMAC sites.
Software used at the sites: Visual FoxPro, FileMaker Pro and Stata
Hardware: PCs, Palm pilots and Laptops. Currently piloting with the Palm pilot.
Lack of qualified staff at some sites to handle Data, in such cases the clinicians or lab based scientists do all the data management.
There are no LANs in Gabon and Gambia SMAC sites.
Telcom problems limiting information exchange.

Future works: With better data communication there are plans to set up a central web based database which can be directly updated from the sites.

Security - David Indome & David Bell

Proxy = local caching of WebPages. Saves b/w and enables control of access to the Web. Also downloads sites that are expected to be visited later, *active caching*. Proxy servers can be *distributed* to improve performance and they can be *chained*, like what we do with the Redwing / NLM NetPilot proxy. Most proxy server products allow Internet *access control*.
Packet filtering: some proxy server products allow packet filtering. This allows them to be used as a *firewall*.
Viruses take major resources to prevent and / or fight.
Virus Protection: user information, on-line scanners on email server and on-line scanners on local machines
Pattern file updates: important! Too many users forget to do the update. Your software is as good as the latest update! Automatic updating systems are the best.
VPN: secure pipeline into your network from elsewhere. Includes tunneling, authe, encryption
Backups: essential! Local or on / through the network. The 'Golden Image' is a full mirror of
Also: full backup, incremental backup and differential backup.

NetPilot is a firewall, mail server, email virus scanner, FTPserver, file server, DNS server, proxy server and probably also makes coffee. VPN from a single machine to the inside is possible, but from the inside to the outside is *not* possible.
Obviously this is an important machine. There are backup systems, like a shelf spare. Access control can be done by user name, group, and time of day.
An extra firewall at a site would only be necessary to protect that site from the other sites.

Security problems encountered – Site presentations

Kisian: Email server used for spamming relay. Nimda infection
→ Implemented Cisco PIX firewall; Antigen for Exchange, updates to server OS's to enhance security. In WRAIR forced logon after 3 minutes idle.
Kilifi: Novell servers have not been infected. Nimda infection on the clients. Email relaying through the Groupwise email software.
→Implemented anti-virus software for email, but not working perfectly.
NIMRI: spam relay, Nimda.
Nairobi: virusses have been problematic. IIS and FTP automatically enabled when installing W2k etc. Outside user got in and used a machine to download files.
→ McAfee Groupshield.
Ifakara: virusses.
→ NAV on local machines. DB server only online when update is necessary.
Amani: virus infections (Sircam).
Noguchi: virus infections. Spamming.
Navrongo: virus infections (Sircam, Nimda). Spamming.
→ NAV
Mbita: spam relay. Virus infection.
Entebbe: Virusses. Misuse of user accounts. Hacking problem into a server.
→ IIS lockdown tool. Antigen. NAV.
Malawi: no problems yet. Possible untoward protocols on the network.
→ NAV, also for email scanning.

General:
BTW: Netpilot will prevent any mail / spam relay.
Virus alerts: what you get, check it against the hoax lists and, if valid, send it to the MIMcom tech list.

MIMcom Network Performance Evaluation - Mike Gill / Inga van Schayk / Greg Romaniak

- IS: see text on flipover sheet Tom. Emphasis on the use of the network and the impact it has had on the work in the site
- MG: see copy of presentation
- GR: see copy of presentation. Describes all the technical reasons for delays on a user-to-webserver link and comments on what can be done about that, if anything. Goal is to maximize the potential of the existing link. Needs a contact person and a workstaion that is always on and available for remote use. gromaniak@igillc.com (http://www.igillc.com)

Site problems

Entebbe: Power. Lightning. Mail routing because of the sync with CDC Atlanta. Leased line routing problem. Downloads from the Internet: users doing things on their own and are not trainable. Music etc downloads. Users storing important docs on the local HDU.

Mbita: Wiring was done badly. The common user problems. Training of users is necessary. Power. Lightning.

Kisian: Power. Lightning. Telephones sometimes down. Automatic virus updates (both download to server and push to clients) not running OK. Internet down through MegaPac ethernet port down. Exchange server running out of disk space. Central UPS down. Connector loose at the back of the C-5. Lots of construction related problems. Virusses brought in by users on diskettes.

Noguchi: Tree in front of VSAT needs trimming. Common user problems.

Nairobi: Internet misuse. Users trying to do things on their own, messing up the network. Unknown problem with wireless, fixable by resetting the AP. Unknown problem with wired machines loosing connection with the domain controller, but not wireless. User education necessary. Common user problems/ user ignorance. Not enough IP addresses for the WRAIR/KEMRI section. Problem with wireless link to WT was fixed. Virus problems.

Kilifi: Relay of spam. Server becoming too small. Backups not running OK. Novell and Windows together. DNS going down. RAS not working. Routing table problem, still advertising a 212.158.87.0 network.

Blantyre: New and growing network, running out of IP addresses. Broadcasts on network that shouldn't be there? Users training necessary, working well. Lots of pre-network existing shares. Support staff shortage. Power. Workstaions sometimes not able to see the domain. Proxy disallowed all users to get to the Internet. ISP slow in responding to problems.

Navrongo: Power. Main UPS dead. Misuse of the Internet link. Access from outside to mail.

Dar: Breezecom link to Internet down for 3 months. MultiVoIP not working. Nimda.

Ifakara: Server hanging problem resolved. User problems. Link usage problems. IT staff shortage. Power.

Amani: Server problems! UPS problems. Power supply for server. No system admin. Outside power supply very unreliable.

DAY 3

Whose problem is this? - Mark Bennett

Problem demarcation – see presentation / hand-out

1st line: sites for all local issues
2nd line: Redwing for the link and the onward Internet connection
Africonnect for technical coordination
NLM for project management and funding coordination

Necessity for formalisation of support

Need to do:

- define who is resp for each area of support
- agree to better methods of reporting
- task allocation

In all cases report issues to the MIMcom helpdesk reporting system. There will be a copy to the Redwing helpdesk mail box.

Mimcom Listserv

Extra support issues:

- Get assistance for Novell or Windows
- Service agreements
- Spares readily available
- VoIPs in more places like NLM, WRAIR, CDC, AfriConnect
- Database management
- Emergency procurement support

Troubleshooting a LAN - Joseph Kaduda
Ppt presentation to be submitted by JK.
Troubleshooting - Anthony Ojwang
Based on the MIMCom troubleshooting document

Redwing helpdesk
NOC: VoFR 2029 / land line +44 1707 621 262

Online Resources - by Inga van Schayk
MIMcom homepage
Docline: Document Delivery Request
Pubmed
MedlinePlus
HINARI (not yet ready for access by more than one machine per site)

DAY 4

Proxy setup
Minimumreqiurements for a P 133 MHz is 64 MB RAM.
Cache size depends on disk size should be at least 10 MB.

Proxy installation demo by Fred Orwa.
Internet Security and Acceleration (ISA) Management
Setting caching parameters.
Access denial to selected sites

ISA must be bought separately but you don't need to buy multiple licences. Academic pricing is about US$ 1,200.
Winproxy, Wingate, Whizzbee (www.whizzbee.com) etc are freeware with a limited trial period. However the free ware should be used with caution since there's no warranty on such software.

Mbita, Noguchi and Kilifi are behind proxy servers.

Cabling presentation by Winston Olwande:

- Essential equipment for crimping, cutting and testing patch cables.
- Cable crimping demo (4-pair strand STP cable).
- Demo on use of a cable tester.
- Cables can be damaged by strain.
- Data (Cable) Analyzer can be used to detect damage on the cable, but the equipment is quite expensive
- A cable tester with an RJ-45, RJ-11 and BNC connectors cost about US$ 100

KEMRI, WT-Nairobi, Ifakara don't have cable testers.

Troubleshooting wireless link by Anthony Ojwang:

Insert the PCMCIA card into the slot the correct way.
Configurations should be right
WEP (Wireless Equivalent Privacy) is a 40 bit key algorithm IEEE standards
Location of desktop PCs fitted with wireless cards is important for top performance.
One could also consider using an antenna attached to the PC using a USB cable.
The access point should be reasonably high.

Patches and software updates - Joseph Kaduda
First of all: even if something is available, do you want or need it? Can it mess up your services or cost you a lot of downtime to implement it? Remember the saying "If it ain't broken, don't fix it".
If you decide to do it, think of the following. Warn users before you start. Make a backup of data and/or email. Do non-critical servers first.
If possible, testing should be done on a non-active server, meaning that you shouldn't do it on a production machine where users expect their data to be. Smaller sites, however, will not have this option. A good backup is then essential.
If you can't do it during working hours, don't even try it. Aim for the evening or a weekend day so you have the time to fix any problems that occur or roll back the whole thing when it really causes major trouble.
But it's better preventing problems. Read any documentation that is on the Internet about the the patch before you start. Microsoft has lots of info on their patches. Novell has TID's, Technical Information Document.
Most patches, round-ups and service packs, be it from Microsoft or Novell Netware, include the previous ones on that particular product. That means you only have to apply one patch/update to get all the previous ones. But sometimes that means it has implications for

other parts of the product, where you don't have any urge to put any patch and sometimes it even necessitates applying other patches or doing upgrades. Read the docs first!

Some patches need to be re-applied after each change on the machine. The doc will explain that and also tell you after which canges it needs to happen.

A big dillemma is also what to download and what not. There are numerous patches etc available. Both Microsoft Baseline Security Analyzer and the MS Critical Updates service recommend many MB's worth of updates every week. It would cost a lot of bandwidth if every user would download that on his/her own. It's better to centralize that, one machine downloads it and other take it from there.

MBSA is a great tool to scan a machine or a range of machine for security holes. It might not be as critical anymore with most sites behind the NetPilot firewall, but it still good to have

Active Directory - Steve Ntabo
AD is a central component to W2k, a switchboard for the resources in the network. It has info about the file storage, security/authentication&authorization etc. It's a central point to manage the servers and services. It is an improvement on the NT4 domain concept.

Router config - Alex Sio
As example a Cable/DSL router is show, but the general concept is the same for all of them. You have to tell the router what the networks are that it will see and where it should route packets that come in from those networks. (i.e. configure it). This is called *static routing*. In some cases it is enough to use *dynamic routing* which means the router looks around and figures out what it should route where.
Some routers can do more than routing, like DHCP or firewall-like services: packet and port filtering, NAT or PAT.

DAY 5

Sites' Websites
Very nice sites all around.
One issue is having a site hosted at in a site. Because of the way the VSAT is set up, hosting a website at a site, so at the end of the satellite link, is not a good idea. The downloads of the page from the outside are going over the smaller bandwidth pipe. Also, you can't put anything on a site that is copyrighted.

UPS – Winston Olwande
The main lesson that everybody should learn is that you never should overload a UPS. In the presentation id described the way to calculate the maximum load in Watts for a UPS, the more you stay under that, the longer the UPS will last.

Netmeeting/Remote Desktop Sharing vs. Terminal Services by Steve Ntabo
(NM to 172.16.11.200, NM to 172.16.11.7 , TS to 172.16.15.11)

Loose issues
The new listserv system (send to listserv@mimcom.net a message with just in the body "SUBSCRIBES SYSOPS")
VOFR numbers: it would be best to hook your VoFR system up to your PABX if you have one.

Documentation
A number of docs are ready. A whole number are in preparation, see Mark's presentation. There is also a set of site descriptions, about 20pages per site. Everything is available on the Intranet.

Users – All sites contribute:

- User's psychology. Who is your most difficult user and why? Folks who want impossible things and complain when it can't work and don't want to know/learn about it.

  Lab technologists are viewed as the most difficult in Entebbe. They are generally stubborn and will always raise unnecessary alarm.

  In Navrongo, the incompetent users who never follow the correct procedures for reporting faults are the most difficult.

  In Nairobi, the most difficult users are from KEMRI, they ask for support and want immediate response irrespective of whether the sysop is busy or not. Also users who cannot articulate their problems and start getting impatient when you can't solve their perceived problem immediately.

  Some solutions:

  Information to the users helps ease the tension. Before downing the server or interrupting the systems operation, it makes a big difference to inform the users well in advance.

  Keep your head; an irritated sysop is not very helpful to the user.

  Users remember the down times, but rarely recall the up time. It is sometimes necessary to show them instances of other systems which also go down. Eg. Oxford, CDC Atlanta and other organizations.

  Keeping a log of the times the link or the intranet go down as a backup to discussions with users.

  A free helpdesk is available on www.Liberum.org

Workshop Evaluation:

Most of the points raised as the workshop's objectives set at the start of the week have been met with exception of two, namely: *Configuring routers and Active Server Pages*. A practical session has been proposed for the next workshop to cover router configuration. The web based databases presentation to be sent out to the users.

One participant had hoped that the workshop will come up with some policies to form the basis of the next workshop. There was a general agreement to come up with some draft policies which sites can use in addition to their existing ones. As part of policy implementation, advertisements have been disabled.

The seminar room was small and did not have the best sound effects. Apart from that, participants were happy with the facilities and found the workshop very interactive, interesting and useful.

****

Proposal to hold the sysop's meeting every year. However, cost, absence from site and length of time to come up with sufficient information to present, should be considered when discussing the frequency of future meetings.

Meeting held on Wednesday 12 June to discuss Nairobi Problems:

- Is the router being reset all the time or not? RSS seems to see that it is, while Steve and Alex are not reseeting it by hand. The router itself could be doing it automatically. Since we can't tell now,
- KEMRI users restriction is necessary. Recent attempt failed because of lack of a policy. There should be a clear policy and memo from Dr.Koech when this is implemented, to inform the users why and how this is happening, but also to protect the support staff.
- B/W: LoC and WT are not paying. they should. Dr.Martin should get in touch with them. and discuss this.
- Meeting Erik with Dr. Kofi and Dr. Koech, Ngumo and Dr. Martin. Purpose is to make them aware about the b/w issue, about all the misuse that is going on. If misuse will continue, b/w needs to increase and KEMRI should pay for that.